PCT/JP2004/011831

日本国特許庁
JAPAN PATENT OFFICE

20.08.2004

REC'D 16 SEP 2004
WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月２８日

出願番号
Application Number: 特願２００３－３０４８８２
[ST. 10/C]: [ＪＰ２００３－３０４８８２]

出願人
Applicant(s): 日本アイ・ビー・エム株式会社

２００４年　６月　７日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００４－３０４９０６２

【書類名】　特許願
【整理番号】　JP9030171
【提出日】　平成15年 8月28日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 19/00
【発明者】
　【住所又は居所】　東京都港区六本木三丁目２番１２号　日本アイ・ビー・エム株式会社内
　【氏名】　石垣　良信
【発明者】
　【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
　【氏名】　沼尾　雅之
【発明者】
　【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
　【氏名】　百合山　まどか
【発明者】
　【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
　【氏名】　渡邊　裕治
【特許出願人】
　【識別番号】　592073101
　【氏名又は名称】　日本アイ・ビー・エム株式会社
【代理人】
　【識別番号】　100086243
　【弁理士】
　【氏名又は名称】　坂口　博
【代理人】
　【識別番号】　100091568
　【弁理士】
　【氏名又は名称】　市位　嘉宏
【代理人】
　【識別番号】　100108501
　【弁理士】
　【氏名又は名称】　上野　剛史
【復代理人】
　【識別番号】　100104880
　【弁理士】
　【氏名又は名称】　古部　次郎
【選任した復代理人】
　【識別番号】　100118201
　【弁理士】
　【氏名又は名称】　千田　武
【手数料の表示】
　【予納台帳番号】　081504
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1

【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0004471
【包括委任状番号】　0004470
【包括委任状番号】　0208086

【書類名】特許請求の範囲
【請求項１】
属性情報が格納されたデータベースから所定の属性情報をネットワークを介して提供する属性情報提供サーバであって、
ネットワークを介して接続されるユーザ装置により、データベースに格納されている属性情報の中から幾つかの属性情報の抜き出し指示を受ける手段と、
前記ユーザ装置によって指示されデータベースから抜き出された前記幾つかの属性情報だけを仮想レコードとしてデータベースに登録する手段と、
前記仮想レコードのキーとしての仮想ＩＤを前記ユーザ装置に提供する手段と、
ネットワークを介して接続される属性情報受信装置から、前記仮想ＩＤを用いた前記仮想レコードの読み込み要求を受ける手段と、
前記属性情報受信装置に対して前記仮想レコードを提供する手段とを含む属性情報提供サーバ。
【請求項２】
前記抜き出し指示を受ける手段は、前記ユーザ装置だけに当該ユーザ装置の操作者に関する属性情報を参照させ、前記仮想レコードを抜き出させる際に、任意の属性に対するコピーを許可する一方、任意の属性に対する改ざんを禁止することを特徴とする請求項１記載の属性情報提供サーバ。
【請求項３】
前記読み込み要求を受ける手段は、データベースの中からどの仮想ＩＤに対する仮想レコードの読み込み要求がなされているかを知り得ない状態にあることを特徴とする請求項１記載の属性情報提供サーバ。
【請求項４】
データベースに格納される属性情報の中から選択された所定の情報である仮想レコードを生成する生成手段と、
前記仮想レコードのキーとなる仮想ＩＤに対応付けてデータベースに格納する格納手段と、
ネットワークを介して接続されるユーザ装置に前記仮想ＩＤを提供する仮想ＩＤ提供手段と、
ネットワークを介して接続される属性情報受信装置からの前記仮想ＩＤを用いた要求に基づいて、当該属性情報受信装置に前記仮想レコードを提供する仮想レコード提供手段とを含み、
前記仮想レコード提供手段は、データベースの中からどの仮想ＩＤが選ばれたかを知り得ない状態にて、当該属性情報受信装置に前記仮想レコードを提供することを特徴とする属性情報提供サーバ。
【請求項５】
前記生成手段は、データベースに格納されている加入者の属性情報の中から、前記ユーザ装置によって抜き出された情報を仮想レコードとして生成することを特徴とする請求項４記載の属性情報提供サーバ。
【請求項６】
前記仮想レコード提供手段は、1-out-of-N OT(Oblivious Transfer)のプロトコルを用いて、前記属性情報受信装置に前記仮想レコードを提供することを特徴とする請求項４記載の属性情報提供サーバ。
【請求項７】
顧客ごとに、複数の属性情報を含む顧客レコードを格納するデータベースと、
顧客が操作するユーザ装置からの要求に基づき、前記データベースから当該顧客の顧客レコードを読み出し、ネットワークを介して前記ユーザ装置に提供する顧客レコード表示部と、
前記ユーザ装置からネットワークを介し、前記顧客レコードの中から所定の属性情報に対する選択を受ける属性選択部と、

前記属性選択部により受けた選択に基づき、前記顧客レコードの中から選択された属性情報によって仮想レコードを生成すると共に、生成された当該仮想レコードを前記データベースに格納する仮想レコード生成部と、

前記仮想レコード生成部により生成された前記仮想レコードを特定するための仮想ＩＤを前記ユーザ装置に提供する仮想ＩＤ発行部とを含む属性情報提供サーバ。

【請求項８】

属性情報受信装置からネットワークを介してなされる前記仮想ＩＤを用いた情報参照要求に基づき、前記データベースから該当する仮想レコードを読み出して当該属性情報受信装置に提供する仮想レコード参照処理部を更に備えたことを特徴とする請求項７記載の属性情報提供サーバ。

【請求項９】

前記仮想レコード生成部は、オリジナルである前記顧客レコードの属性内容と、生成された前記仮想レコードの属性内容とを比較し、改ざんされていないことを検証することを特徴とする請求項７記載の属性情報提供サーバ。

【請求項１０】

前記仮想ＩＤ発行部により前記ユーザ装置に提供される前記仮想ＩＤは、前記顧客レコードのＩＤとはアンリンカブルなＩＤであることを特徴とする請求項７記載の属性情報提供サーバ。

【請求項１１】

複数の属性情報を含むレコードを格納するレコード格納手段と、

前記レコード格納手段により格納された前記レコードの中から、ネットワークを介して選択された所定の属性情報によって生成された仮想レコードを格納する仮想レコード格納手段と、

どの仮想レコードが選ばれたかを知り得ない状態にて、前記仮想レコード格納手段の中から選ばれた仮想レコードを、ネットワークを介して開示する仮想レコード開示手段とを含む属性情報提供サーバ。

【請求項１２】

前記仮想レコード格納手段は、キーとしての仮想ＩＤに対応付けて仮想レコードを格納し、

前記仮想レコード開示手段は、どの仮想ＩＤが選ばれたかを知り得ない状態にて、前記仮想ＩＤを用いた開示要求を受けることを特徴とする請求項１１記載の属性情報提供サーバ。

【請求項１３】

前記仮想レコード開示手段は、オブリビアストランスファー(Oblivious Transfer)の暗号技術を用いて前記仮想レコードの開示を実現することを特徴とする請求項１１記載の属性情報提供サーバ。

【請求項１４】

ネットワークを介してなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出すステップと、

読み出された前記所定のレコードを、ネットワークを介して前記ユーザ装置に提供するステップと、

前記所定のレコードの中から所定の属性情報に対する前記ユーザ装置からの選択をネットワークを介して受けるステップと、

前記所定のレコードの中から選択された前記所定の属性情報を含む仮想レコードを生成するステップと、

生成された前記仮想レコードをデータベースに格納するステップと、

格納された前記仮想レコードを特定するための仮想ＩＤをネットワークを介して前記ユーザ装置に提供するステップとを含む属性情報提供方法。

【請求項１５】

ネットワークを介して属性情報受信装置から前記仮想ＩＤを用いた情報参照要求を受け

るステップと、
前記情報参照要求に基づき、データベースから該当する仮想レコードを読み出すステップと、
読み出された前記仮想レコードを前記属性情報受信装置にネットワークを介して提供するステップとを更に含む請求項１４記載の属性情報提供方法。
【請求項１６】
前記情報参照要求は、1-out-of-N OT(Oblivious Transfer)のプロトコルを用いてなされることを特徴とする請求項１４記載の属性情報提供方法。
【請求項１７】
データベースに格納される前記仮想レコードの属性情報が前記顧客レコードの属性情報から改ざんされたものでないことを検証するステップを更に含む請求項１４記載の属性情報提供方法。
【請求項１８】
顧客別の顧客レコードの中から所定の属性が選択されて生成された仮想レコードをキーとなる仮想ＩＤに対応付けて格納されたデータベースに対して、当該仮想ＩＤを用いた当該仮想レコードの取得要求を受けるステップと、
前記仮想ＩＤに対応する前記仮想レコードを前記データベースから読み出し、前記取得要求に対して当該仮想レコードを開示するステップとを含み、
前記仮想レコードの取得要求を受けるステップは、当該取得要求を受ける際に、どの仮想ＩＤが選ばれたかが秘匿されることを特徴とする属性情報提供方法。
【請求項１９】
顧客自身のコンピュータ装置を介して、当該顧客自身の顧客レコードの中から所定の属性の選択を受けるステップと、
選択された前記所定の属性だけを属性とする前記仮想レコードを生成して前記データベースに格納するステップと、
前記データベースに格納された前記仮想レコードのキーとなる前記仮想ＩＤを前記コンピュータ装置に提供するステップとを更に含む請求項１８記載の属性情報提供方法。
【請求項２０】
ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能するコンピュータに、
ネットワークを介してなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出す機能と、
読み出された前記所定のレコードを、ネットワークを介して前記ユーザ装置に提供する機能と、
前記所定のレコードの中から所定の属性情報に対する前記ユーザ装置からの選択をネットワークを介して受ける機能と、
前記所定のレコードの中から選択された前記所定の属性情報を含む仮想レコードを生成する機能と、
生成された前記仮想レコードをデータベースに格納する機能と、
格納された前記仮想レコードを特定するための仮想ＩＤをネットワークを介して前記ユーザ装置に提供する機能とを実現させるプログラム。
【請求項２１】
前記コンピュータに、データベースに格納される前記仮想レコードの属性情報が前記レコードの属性情報から改ざんされたものではないことを検証する機能を更に実現させる請求項２０記載のプログラム。
【請求項２２】
ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能するコンピュータに、
格納されるレコードの中から所定の属性が選択されて生成された仮想レコードを、キーとなる仮想ＩＤに対応付けてデータベースに格納する機能と、

どの仮想ＩＤが選ばれたかが秘匿された状態にて前記仮想ＩＤを用いた前記仮想レコードの取得要求を受ける機能と、

前記仮想ＩＤに対応する前記仮想レコードを前記データベースから読み出し、前記取得要求に対して当該仮想レコードを開示する機能とを実現させるプログラム。

【書類名】明細書
【発明の名称】属性情報提供サーバ、属性情報提供方法、およびプログラム
【技術分野】
【０００１】
本発明は、ネットワークを介して属性情報を提供する属性情報提供サーバ等に関する。
【背景技術】
【０００２】
属性証明書(Attribute Certificate)は、通常の公開鍵証明書が本人性を証明するのに対して、その人物がユーザ権限として、どのような属性を持っているかを証明するものであり、ＩＥＴＦ(Internet Engineering Task Force)の定めるＸ．５０９でその仕様が定められている(例えば、非特許文献１参照。)。また、発行も公開鍵証明書を発行する公開鍵認証局(Certification Authority)ではなく、属性認証機関(Attribute Authority)によって行われる。このように、本人性と属性との認証を分ける動きは、ＯＡＳＩＳ(構造化情報標準促進協会)の標準であるＳＡＭＬ(Security Assertion Markup Language)でも取り入れられており、複数の独立機関によるドメインをまたがった柔軟な認証・許可を可能にし、Federated ＩＤという新しい認証サービスの提案にもつながっている(例えば、非特許文献２参照。)。
【０００３】
この属性情報(属性データ)には、氏名、住所、年齢、職業、電話番号、性別、家族構成などが含まれるが、これらの属性情報の中には、会社の人事部が証明するような組織上の職位に関するようなものから、個人の趣味のようなものまで様々なものがある。前述の属性証明書が使えるものは、属性自身が公的第三者によって証明できるようなものであり、プライバシー保護の観点から、趣味のような個人的な属性には第三者機関を認証機関とするのは適さない。このように、属性には、第三者から認定されるAuthorized属性と、完全に個人の任意で決められるDiscretionary属性があり、それぞれ異なるセキュリティ要件がある。
【０００４】
ここで、属性データを与信情報として扱うものとして、ＩＣチップ付きのクレジットカード内に、カード番号以外に住所などの属性情報を入れておくことで、商店などにてクレジット決済の際に付加情報を同時に開示できる従来技術が存在する(例えば、特許文献１参照。)。かかる特許文献１では、付加情報を区分化し、情報の開示レベルによってこの開示する情報をコントロールする機能についても示されている。また、クレジット会社などの運営する信用センターが、各加盟店の信用レベルを格付けし、それによって情報開示レベルを決定する機能についても示されている。
【０００５】
また、ネットワークを介しての通信における認証システムにて、認証サーバが新規の登録者に対して共通ＩＤであるユニバーサルＩＤを発行し、このユニバーサルＩＤを提示した要求に応じて、他の端末者に対して登録者の個人情報から住所などの商取引に必要な情報を抽出して送信することで、ネットワークを介して商品の購入やサービスの提供を受ける際に必要とされる個人情報の入力操作を簡略化する技術が開示されている(例えば、特許文献２参照。)。
【０００６】
【非特許文献１】FC 3281 on An Internet Attribute Certificate [平成１５年８月４日検索] インターネット<http://www1.ietf.org/mail-archive/ietf-announce/Current/msg18344.html>
【非特許文献２】Liberty Alliance [平成１５年８月４日検索] インターネット<http://www.projectliberty.org/>
【特許文献１】特開２００１－３２５５２６号公報(第４－５頁、図１)
【特許文献２】特開２００１－２４４９２７号公報(第３－４頁、図１)
【発明の開示】

【発明が解決しようとする課題】

【０００７】

ところで、前述したAuthorized属性の中で、例えば預金残高や購買履歴、会員情報などといった、個人とそれが属するサービスプロバイダとの共有情報についても、その個人の属性として扱えると便利なことが多い。例えば米国においては、カード取得のための審査はかなり厳重で、例えば、１年以上、銀行口座を管理していたという取引履歴が必要とされる。かかる場合に、その取引銀行から認証をしてもらえれば、新規取引が容易となり、加入者にとってもサービスプロバイダにとっても、利のあるサービスとなり得る。こうした共有情報は、本来は個人の情報として保護されるべきものであるが、個人の同意と希望のもとに、かかる情報を、それを保護するサービスプロバイダに認証してもらう個人属性与信サービスの仕組みが望まれるところである。

【０００８】

また、与信をサービスとするビジネスとしては、クレジットカードが代表的なものであるが、ここでは、与信額を上限とする金銭を与信の対象として、クレジットカード会社の加入者が加入店舗から商品を購入するときの決算サービスが行われている。ところが、インターネットのようなネットワーク上では、お互いに全く知らないもの同士が取り引きを開始したい場合がある。このようなネットワーク上における与信の特徴として、

１.与信の対象は金銭以外の信頼情報であること。

２.取り引きをしようとする二者は必ずしも同じ信頼機関に属していないこと。

等が挙げられる。そのために、クレジットカードの仕組みでは実現できない、金銭以外で与信になるものとして、信頼できる組織の会員(membership)であることや、その会員として所属する期間、その間の活動履歴などが重要となる。これらは、全て個人とその所属する機関が共有する情報である。また、信頼熟成のためには、取り引きをしようとしている二者が同じ組織に属している必要はなく、それぞれが備えている基準に照らして、相手を信頼できるかどうか決定できるような仕組みが必要である。現在のクレジットカードの仕組みでは、責任、与信範囲、および取引対象者が予め決められており、こうしたネットワーク上で期待されているようなフレキシブルな与信付与の仕組みは実現されていない。

【０００９】

更に、上述した特許文献１に記載の技術では、参加者が従来のクレジットカードの枠組みに制限されており、また、その属性も商店が商品を配送するために必要な情報に限定されている。また、上述したＸ.５０９等の属性証明のための技術では、例えば非特許文献１等では属性証明書のフォーマットを決めているだけであり、具体的なサービスの仕組みについてはカバーされていない。また更に、上述した特許文献２に記載の技術では、加入者の匿名性やどの属性を証明するか等について、加入者自身がコントロールすることができない。また、自分がどの新規取引業者と取り引きしようとしているかを個人情報取り扱い業者に常に認識されることから、加入者にとっては十分なプライバシーの保護が図られない。

【００１０】

本発明は、以上のような技術的課題を解決するためになされたものであって、その目的とするところは、インターネットなどのネットワークを用いて、例えば金銭以外の属性を与信の対象とすること等を可能とする属性情報提供サービスを実現することにある。

また他の目的は、加入者の個人情報の一部を、加入者の同意の下で、新規取引者に提供することにある。

更に他の目的は、加入者がどの新規取引業者と取り引きしようとしているかを個人情報取り扱い業者に知られずに、認証を可能とすることにある。

【課題を解決するための手段】

【００１１】

かかる目的のもと、本発明は、属性情報が格納されたデータベースから所定の属性情報をネットワークを介して提供する属性情報提供サーバであって、ネットワークを介して接続されるユーザ装置により、データベースに格納されている属性情報の中から幾つかの属

性情報の抜き出し指示を受ける手段と、ユーザ装置によって指示されデータベースから抜き出された幾つかの属性情報だけを仮想レコードとしてデータベースに登録する手段と、仮想レコードのキーとしての仮想ＩＤをユーザ装置に提供する手段と、ネットワークを介して接続される属性情報受信装置から、仮想ＩＤを用いた仮想レコードの読み込み要求を受ける手段と、属性情報受信装置に対して仮想レコードを提供する手段とを含む。

【００１２】

ここで、この抜き出し指示を受ける手段は、ユーザ装置だけにユーザ装置の操作者に関する属性情報を参照させ、仮想レコードを抜き出させる際に、任意の属性に対するコピーを許可する一方、任意の属性に対する改ざんを禁止することを特徴とすることができる。これによれば、属性情報提供サーバは、自らがユーザ装置との間で得た活動履歴などの個人情報の一部を、加入者であるユーザ装置の同意の下で、属性情報受信装置に開示する際、それが改ざんされていないということだけを責任範囲として、与信をする仕組みを提供できる。また、読み込み要求を受ける手段は、データベースの中からどの仮想ＩＤに対する仮想レコードの読み込み要求がなされているかを知り得ない状態にあることを特徴とすることができる。

【００１３】

一方、本発明が適用される属性情報提供サーバは、データベースに格納される属性情報の中から選択された所定の情報である仮想レコードを生成手段によって生成し、この仮想レコードのキーとなる仮想ＩＤに対応付けて格納手段によりデータベースに格納する。また、ネットワークを介して接続されるユーザ装置に仮想ＩＤ提供手段により仮想ＩＤを提供し、ネットワークを介して接続される属性情報受信装置からの仮想ＩＤを用いた要求に基づいて、仮想レコード提供手段は、属性情報受信装置に仮想レコードを提供する。この仮想レコード提供手段は、データベースの中からどの仮想ＩＤが選ばれたかを知り得ない状態にて、属性情報受信装置に仮想レコードを提供することを特徴とすることができる。

【００１４】

ここで、この生成手段は、データベースに格納されている加入者の属性情報の中から、ユーザ装置によって抜き出された情報を仮想レコードとして生成することを特徴とすることができる。また、この仮想レコード提供手段は、1-out-of-N OT(Oblivious Transfer)のプロトコルを用いて、属性情報受信装置に仮想レコードを提供することを特徴とすることができる。

【００１５】

他の観点から把えると、本発明が適用される属性情報提供サーバは、顧客ごとに、複数の属性情報を含む顧客レコードを格納するデータベースと、顧客が操作するユーザ装置からの要求に基づき、データベースから顧客の顧客レコードを読み出し、ネットワークを介してユーザ装置に提供する顧客レコード表示部と、ユーザ装置からネットワークを介し、顧客レコードの中から所定の属性情報に対する選択を受ける属性選択部と、この属性選択部により受けた選択に基づき、顧客レコードの中から選択された属性情報によって仮想レコードを生成すると共に、生成された仮想レコードをデータベースに格納する仮想レコード生成部と、この仮想レコード生成部により生成された仮想レコードを特定するための仮想ＩＤをユーザ装置に提供する仮想ＩＤ発行部と、属性情報受信装置からネットワークを介してなされる仮想ＩＤを用いた情報参照要求に基づき、データベースから該当する仮想レコードを読み出して属性情報受信装置に提供する仮想レコード参照処理部とを含む。

【００１６】

ここで、この仮想レコード生成部は、オリジナルである顧客レコードの属性内容と、生成された仮想レコードの属性内容とを比較し、改ざんされていないことを検証することを特徴としている。また、この仮想ＩＤ発行部によりユーザ装置に提供される仮想ＩＤは、顧客レコードのＩＤとはアンリンカブルなＩＤであることを特徴とすることができる。

【００１７】

また、本発明が適用される属性情報提供サーバは、複数の属性情報を含むレコードをレコード格納手段により格納し、このレコード格納手段により格納されたレコードの中から

、ネットワークを介して選択された所定の属性情報によって生成された仮想レコードを仮想レコード格納手段により格納する。そして、どの仮想レコードが選ばれたかを知り得ない状態にて、仮想レコード格納手段の中から選ばれた仮想レコードを、仮想レコード開示手段によりネットワークを介して開示する。

【００１８】

ここで、この仮想レコード格納手段は、キーとしての仮想ＩＤに対応付けて仮想レコードを格納し、仮想レコード開示手段は、どの仮想ＩＤが選ばれたかを知り得ない状態にて、仮想ＩＤを用いた開示要求を受けることを特徴としている。より具体的には、この仮想レコード開示手段は、オブリビアストランスファー(Oblivious Transfer)の暗号技術を用いて仮想レコードの開示を実現している。

【００１９】

一方、本発明を方法のカテゴリから把えると、本発明が適用される属性情報提供方法は、ネットワークを介してなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出すステップと、読み出された所定のレコードを、ネットワークを介してユーザ装置に提供するステップと、所定のレコードの中から所定の属性情報に対するユーザ装置からの選択をネットワークを介して受けるステップと、所定のレコードの中から選択された所定の属性情報を含む仮想レコードを生成するステップと、生成された仮想レコードをデータベースに格納するステップと、データベースに格納される仮想レコードの属性情報が顧客レコードの属性情報から改ざんされたものでないことを検証するステップと、格納された仮想レコードを特定するための仮想ＩＤをネットワークを介してユーザ装置に提供するステップと、ネットワークを介して属性情報受信装置から仮想ＩＤを用いた情報参照要求を受けるステップと、この情報参照要求に基づき、データベースから該当する仮想レコードを読み出すステップと、読み出された仮想レコードを属性情報受信装置にネットワークを介して提供するステップと、を含む。この情報参照要求は、1-out-of-N OT(Oblivious Transfer)のプロトコルを用いてなされることを特徴とすることができる。

【００２０】

更に他の観点から把えると、本発明が適用される属性情報提供方法は、顧客別の顧客レコードの中から所定の属性が選択されて生成された仮想レコードをキーとなる仮想ＩＤに対応付けて格納されたデータベースに対して、この仮想ＩＤを用いた仮想レコードの取得要求を受けるステップと、仮想ＩＤに対応する仮想レコードをデータベースから読み出し、取得要求に対して仮想レコードを開示するステップとを含み、この仮想レコードの取得要求を受けるステップは、取得要求を受ける際に、どの仮想ＩＤが選ばれたかが秘匿されることを特徴としている。ここで、この顧客自身のコンピュータ装置を介して、顧客自身の顧客レコードの中から所定の属性の選択を受けるステップと、選択された所定の属性だけを属性とする仮想レコードを生成してデータベースに格納するステップと、データベースに格納された仮想レコードのキーとなる仮想ＩＤをコンピュータ装置に提供するステップとを更に含むことができる。

【００２１】

また本発明は、ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能するコンピューがこれらの各機能を実現可能に構成されたプログラムとして把握することができる。このプログラムをコンピュータに対して提供する際に、例えばサーバとしてのコンピュータにインストールされた状態にて提供される場合の他、コンピュータに実行させるプログラムをコンピュータが読取可能に記憶した記憶媒体にて提供する形態が考えられる。この記憶媒体としては、例えばＤＶＤやＣＤ－ＲＯＭ媒体等が該当し、ＤＶＤやＣＤ－ＲＯＭ読取装置等によってプログラムが読み取られ、フラッシュＲＯＭ等にこのプログラムが格納されて実行される。また、これらのプログラムは、例えば、プログラム伝送装置によってネットワークを介して提供される形態がある。

【００２２】

具体的には、本発明が適用されるプログラムは、コンピュータに、ネットワークを介し

てなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出す機能と、読み出された所定のレコードを、ネットワークを介してユーザ装置に提供する機能と、所定のレコードの中から所定の属性情報に対するユーザ装置からの選択をネットワークを介して受ける機能と、この所定のレコードの中から選択された所定の属性情報を含む仮想レコードを生成する機能と、データベースに格納される仮想レコードの属性情報がレコードの属性情報から改ざんされたものではないことを検証する機能と、生成された仮想レコードをデータベースに格納する機能と、格納された仮想レコードを特定するための仮想ＩＤをネットワークを介してユーザ装置に提供する機能とを実現させる。

【００２３】

他の観点から把えると、本発明が適用されるプログラムは、ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能するコンピュータに、格納されるレコードの中から所定の属性が選択されて生成された仮想レコードを、キーとなる仮想ＩＤに対応付けてデータベースに格納する機能と、どの仮想ＩＤが選ばれたかが秘匿された状態にて仮想ＩＤを用いた仮想レコードの取得要求を受ける機能と、仮想ＩＤに対応する仮想レコードをデータベースから読み出し、取得要求に対して仮想レコードを開示する機能とを実現させる。

【発明の効果】

【００２４】

本発明によれば、属性情報を持つ機関が、例えば特定個人の属性情報の一部を第三者に提供することで、例えば特定個人や機関に対して属性情報に関する利益のあるビジネスを提供することができる。

【発明を実施するための最良の形態】

【００２５】

以下、添付図面を参照して、本発明の実施の形態について詳細に説明する。

図１は、本実施の形態が適用される属性情報提供システム(与信付与システム)の全体構成を示した図である。ここでは、個人情報取り扱い業者に設置される属性情報提供サーバ(個人情報サーバ)１０、属性情報提供システムの加入者がクライアント端末として用いるユーザ装置３０、新規取引者が利用するクライアント端末である属性情報受信装置(与信情報受信装置)５０が配置され、これらがインターネット等のネットワーク７０を介して接続されている。このネットワーク７０は、インターネットなどの公的、広域的なネットワークでもローカルなネットワークでも良い。すなわち、インターネット上に設けられた公的なデータベースサーバを属性情報提供サーバ１０として本実施形態のシステムを構築することもできるし、企業内イントラネットのような閉じた形態で本実施形態のシステムを構築することもできる。

【００２６】

サービスプロバイダが管理するサーバである属性情報提供サーバ１０は、会員(ユーザ装置３０)の個人情報や会員との間の取引情報を管理し、会員の同意に基づいて属性を認証するための仮想ＩＤトークン(ＶＩＤトークン)を発行している。仮想ＩＤトークンは、仮想ＩＤ(ＶＩＤ)に、例えば属性情報提供サーバ１０のＵＲＬ等を含んで形成される。この仮想ＩＤの発行依頼者として、サービスプロバイダの会員であるユーザ装置３０では、属性情報提供サーバ１０に登録してある個人情報(顧客レコード、単に「レコード」とする場合がある)から、新規取引者である属性情報受信装置５０に開示したい属性が選ばれ、属性情報提供サーバ１０に対してＶＩＤトークンの発行の依頼がなされる。属性受領者としての任意の相手である属性情報受信装置５０は、ユーザ装置３０との新規取引の際に、信頼関係構築のための属性証明書を属性情報提供サーバ１０経由で受け取っている。

【００２７】

属性情報提供サーバ１０では、加入者であるユーザ装置３０との間でＶＩＤトークンの発行が行われ、また、新規取引者である属性情報受信装置５０との間で仮想レコードの参照が行われる。この中で、ＶＩＤトークンを秘密にしたまま参照するものをＶＩＤ秘匿参

照とする。尚、属性情報提供サーバ１０の機能については、後に詳述する。

【００２８】

ユーザ装置３０では、属性情報提供サーバ１０からのＶＩＤトークンの取得と、それを属性情報受信装置５０に渡すためのＶＩＤトークンの送信が行われる。

このＶＩＤトークンの取得では、ユーザ装置３０は、所定のＷｅｂブラウザを使用して属性情報提供サーバ１０と通信をする。このとき、ＳＳＬ(Secure Sockets Layer)などの暗号化および認証機能を用いることによって、第三者が情報を盗み見ることを防ぐことができる。また、ユーザ装置３０の認証も、通常のＨＴＴＰ(Hypertext Transfer Protocol)で定められているBasic認証などを使うことも可能である。

ＶＩＤトークンの送信では、ユーザ装置３０は、取得したＶＩＤトークンをＳＭＴＰ(Simple Mail Transfer Protocol)などのメールプロトコルを用いて属性情報受信装置５０に送信している。

【００２９】

属性情報受信装置５０では、ユーザ装置３０からのＶＩＤトークンの取得と、属性情報提供サーバ１０からの仮想レコードの取得が行われる。

まず、ＶＩＤトークンの取得では、通常のメールソフトなどによって、ユーザ装置３０からＶＩＤトークンが取得される。

仮想レコードの取得としては、通常取得とＶＩＤ秘匿取得とがある。通常取得の処理では、ＶＩＤトークンに含まれるＵＲＬによって属性情報提供サーバ１０に接続し、ＶＩＤを提示することで、その仮想レコードを取得する。ＶＩＤ秘匿取得では、属性情報受信装置５０と属性情報提供サーバ１０との間で、後述するＯＴプロトコルを行うことで、所定の属性を得ることができる。

【００３０】

本実施の形態では、以下の２つの暗号技術を要素技術として用いている。

まず、第１の暗号技術は、オブリビアストランスファー(ＯＴ:Oblivious Transfer)である。1-out-of-N OTは、Ｎ個の情報を持つサーバと、そのうちの１つを読みたいクライアントの間(２者の間)のプロトコルで、クライアントはＮ個のうち１つだけ情報を読むことができるが、そのどれを読めたかをサーバは知ることができないとするものである。即ち、情報提供者である属性情報提供サーバ１０が持つＮ個の情報のうち、クライアント(例えば、属性情報受信装置５０)は、その１つだけを受け取ることができ、そのどれを選んだかを属性情報提供サーバ１０は知り得ない。尚、詳細は文献[Naor, M. and Pinkas, B.: Oblivious Transfer and Polynomial Evaluation, in proc. of STOC, 1999.]に詳しいが、ここではその内容を省略する。

【００３１】

第２の暗号技術は、暗号関数の準同型性である。準同型性をもつ公開鍵暗号関数Ｅpk(Ｘ)は、

$$Epk1(Epk2(X)) = Epk2(Epk1(X))$$

を満たす。例えば、後述するエルガマル(ElGamal)暗号などは準同型性を有している。

【００３２】

ここで、図１に示す属性情報提供システムにて実行される各プロトコルについて説明する。

図２は、属性情報提供システムの各装置が実行する処理を示したフローチャートである。図１の全体構成図を参照して説明すると、まず、ネットワーク７０を介してユーザ装置３０から属性情報提供サーバ１０に対し、仮想ＩＤ(ＶＩＤ：Virtual ＩＤ)を含む仮想ＩＤトークン(ＶＩＤトークン)の発行依頼が出される(ステップ２０１)。このとき、ユーザ装置３０は、自分の個人情報(顧客レコード)からどれをＶＩＤトークンの下で開示するかを選択する(ステップ２０２)。属性情報提供サーバ１０では、後述するＧＩＤ(Globally-unique ID)から属性の一部がコピーされ、仮想ＩＤをキーとしてデータベース(後述)に登録される(ステップ２０３)。そして、属性情報提供サーバ１０からユーザ装置３０に対して、ネットワーク７０を介してＶＩＤトークンが発行される(ステップ２０４)。

【００３３】
その後、ユーザ装置３０から属性情報受信装置５０に対し、ＶＩＤトークンが渡され、仮想ＩＤを含めた取引依頼がネットワーク７０を介して出力される(ステップ２０５)。その後、属性情報受信装置５０は、属性情報提供サーバ１０に対して取得した仮想ＩＤを提示し、付随する属性情報の開示を要求する(ステップ２０６)。属性情報提供サーバ１０は、仮想ＩＤをキーとする属性を与信情報として、即ち、仮想ＩＤの参照情報(仮想レコード)を属性情報受信装置５０に開示する(ステップ２０７)。このようにして、仮想レコードを取得した属性情報受信装置５０は、開示された属性(仮想レコードの結果)により、新規取引するだけの信頼が得られた場合には、ユーザ装置３０に対してネットワーク７０を介し、取り引きの承諾を通知し、ユーザ装置３０と属性情報受信装置５０との間で取り引きが開始される(ステップ２０８)。

【００３４】
次に、本実施の形態が適用される各構成要素のハードウェア構成について説明する。
図３は、本実施形態の属性情報提供サーバ１０やユーザ装置３０、属性情報受信装置５０を実現するのに好適なコンピュータ装置のハードウェア構成例を模式的に示した図である。
図３に示すコンピュータ装置は、演算手段であるＣＰＵ(Central Processing Unit：中央処理装置)１０１、M/B(マザーボード)チップセット１０２、このM/Bチップセット１０２およびＣＰＵバスを介してＣＰＵ１０１に接続されたメインメモリ１０３、同じくM/Bチップセット１０２およびＡＧＰ(Accelerated Graphics Port)を介してＣＰＵ１０１に接続されたビデオカード１０４を備えている。また、ＰＣＩ(Peripheral Component Interconnect)バスを介してM/Bチップセット１０２に接続された磁気ディスク装置(ＨＤＤ)１０５、およびネットワークインターフェイス１０６を有している。更に、このＰＣＩバスからブリッジ回路１０７およびＩＳＡ(Industry Standard Architecture)バスなどの低速なバスを介してM/Bチップセット１０２に接続されたフロッピーディスクドライブ１０８、およびキーボード/マウス１０９とを備えている。

【００３５】
尚、図３は本実施形態を実現するコンピュータ装置のハードウェア構成を例示するに過ぎず、本実施形態を適用可能であれば、他の種々の構成を取ることができる。例えば、ビデオカード１０４を設ける代わりに、ビデオメモリのみを搭載し、ＣＰＵ１０１にてイメージデータを処理する構成としても良い。また、外部記憶装置として、ＡＴＡ(AT Attachment)やＳＣＳＩ(Small Computer System Interface)などのインターフェイスを介して、ＣＤ－Ｒ(Compact Disc Recordable)やＤＶＤ－ＲＡＭ(Digital Versatile Disc Random Access Memory)のドライブ等を設けることも可能である。

【００３６】
次に、本実施形態の属性情報提供サーバ１０における機能構成を、図４を用いて詳述する。
図４に示すように、属性情報提供サーバ１０は、ＶＩＤ発行の機能として、抜き出し指示を受ける手段として機能する顧客レコード表示部１１および属性選択部１２、仮想レコードの生成手段の一つとして機能する仮想レコード生成部１３、仮想ＩＤ提供手段の一つとして機能するＶＩＤトークン発行部１４を備えている。また、仮想レコードの参照機能(仮想レコード提供手段)として、仮想レコード参照処理部１８および仮想レコード発行部１９を備えている。更に、例えば図３に示す磁気ディスク装置１０５を用いて、加入者であるユーザ装置３０の顧客レコードや仮想レコードを格納するデータベース２０を備えている。

【００３７】
このデータベース２０では、図５に示すようなテーブルで個人情報を管理している。もともとの個人情報のレコードは、顧客ごとに、複数の属性からなる顧客レコードをＧＩＤ(Globally-unique ID)をキーとして保存されている。そして、ここから属性の一部がコピーされたものを、仮想ＩＤをキーとして登録するものとしている。図５に示すように、同

一個人の情報であっても、仮想ＩＤでは、ＧＩＤの属性の異なった一部だけがコピーされており、仮想ＩＤである「Ｖ０１０１０１」と「Ｖ０１００１１」とでは、各々、異なった属性情報が選択されている。仮想ＩＤ属性の属性証明では、不必要な属性にはフィルタがかけられている。また、例えば図５に示す仮想ＩＤ「Ｖ０１００１１」のように、匿名属性として、名前の部分にフィルタをかけることができる。仮想ＩＤの発行に際し、この仮想ＩＤは、ＧＩＤとはアンリンカブル(Unlinkable)なＩＤとされる。また、属性コピーでは、必要な属性のみが実ＩＤであるＧＩＤの属性からコピーされる。尚、仮想ＩＤフィールドは、実ＩＤと全く同等に扱うことができ、属性が欠落した実ＩＤレコードとの区別がつかないように構成されている。

【００３８】

顧客レコード表示部１１は、仮想ＩＤの発行に際し、データベース２０より加入者であるユーザ装置３０の顧客レコードを取り出し、この取り出した内容を、参照のために、例えばユーザ装置３０のディスプレイ(図示せず)に表示する。ここで表示される顧客レコードは、例えば、図５に示したように、プライマリーキーとしてＧＩＤを持ち、名前や住所などの複数の属性からなるレコードである。尚、顧客レコード表示部１１には、図５に示すように、ＧＩＤと共に、今までに所定の属性が選択されて生成された仮想レコードも表示させ、参照させることができる。

属性選択部１２は、加入者であるユーザ装置３０に、表示された属性から、新規取引者である属性情報受信装置５０に提示したい属性だけを抜き出させる(選ばせる)。

【００３９】

仮想レコード生成部１３は、ユーザ装置３０にて抜き出された属性だけをコピーした新しいレコードを作る。このレコードのプライマリーキーとして、既存のレコードのプライマリーキーであるＧＩＤとぶつからないようなＩＤを生成し、これを仮想ＩＤとする。また、ここでは、仮想ＩＤの値が定義されるドメインは、十分に大きいものとし、仮想ＩＤを知らない者が総当り攻撃などで偶然、仮想ＩＤを探りあてることはないものと仮定する。生成された仮想レコードは、データベース２０に格納される。

ＶＩＤトークン発行部１４では、仮想レコード生成部１３によって生成された仮想ＩＤと、自サーバ(属性情報提供サーバ１０)のＵＲＬの組 {ＶＩＤ,ＵＲＬ} とをＶＩＤトークンとして発行する。

【００４０】

仮想レコード参照処理部１８では、仮想レコードの参照に際して、通常参照の処理、またはＶＩＤ秘匿参照の処理が実行される。ＶＩＤトークンをユーザ装置３０から受信した属性情報受信装置５０は、前述のように、例えばブラウザを用いて、ＶＩＤトークンに含まれるＵＲＬにアクセスすることにより、属性情報提供サーバ１０に接続される。仮想レコード参照処理部１８は、属性情報受信装置５０から提示された仮想ＩＤに基づいて、データベース２０から仮想レコードを検索し、仮想レコード発行部１９により、属性情報受信装置５０のディスプレイ(図示せず)に検索結果を表示する。属性情報受信装置５０は、かかる表示によって、仮想レコードにある属性情報を取得することができる。場合によっては、仮想レコード参照処理部１８や仮想レコード発行部１９にて、属性に属性情報提供サーバ１０の署名を付けて、確かに属性情報提供サーバ１０にある属性情報であるということを証明するようなサービスも付加することが可能である。

【００４１】

次に、属性情報提供サーバ１０にて実行される仮想ＩＤ秘匿参照の処理について説明する。

秘匿参照は、仮想ＩＤを属性情報提供サーバ１０に秘密にしたまま仮想レコードを取得するものであり、前述したＯＴ(ObliviousTransfer)が用いられる。以下では簡単なＯＴ、

ＯＴ({s_1,..,s_n})

について説明する。

まず、属性情報提供サーバ１０は、予めランダムに秘密の値 $t_s ¥in Z_q$ を決定し

$Q_0 = g^{t_s} ¥pmod p$
を公開しておく。
属性情報受信装置５０は、秘密鍵 t_u をランダムに Z_q から選び、その公開鍵である
$Q_u = g^{t_u} ¥pmod p$
を計算する。ここで、属性情報受信装置５０は、属性情報提供サーバ１０の h 番目の情報を得ようとしているものとする。このとき、まず、２点 $\{(0, Q_0), (h, Q_u)\}$ を通るような１次多項式 $Y(x)$ を、例えばラグランジュの補間法を使って一意に決定する。この多項式を使って、n 点 $Y_I = Y(i), i=0,..,n-1$ を計算し、$¥{Y_1, Y_2,.., Y_n¥}$ を属性情報提供サーバ１０に送る。
属性情報提供サーバ１０は、属性情報受信装置５０の公開している点が１次多項式上の点であることを検証した後、Y_iをそれぞれエルガマル(ElGamal)暗号の公開鍵として、秘密情報s_iを暗号化したもの $E_y(s_i, Y_i), i=1,..,n$ を属性情報受信装置５０に送る。
属性情報受信装置５０は、h によって指定された点については、それに対応する秘密鍵 t_u を持っているので、属性情報提供サーバ１０から送り返されたElGamal暗号文を復号できる。したがって、１個の秘密情報を得ることが可能となる。

【００４２】

ＯＴでは、ｈ番目を指定しなければならないが、属性情報受信装置５０の持つ仮想ＩＤ(ＶＩＤ)が、全体の顧客レコードの何番目であるのかは、以下のように設定することができる。例えば、属性情報提供サーバ１０は、一方向性ハッシュ関数Ｈ() を用い、Ｈ(ＶＩＤ)のリストを公開することで設定を可能とすることができる。ここで、ハッシュ関数Ｈのアルゴリズムは公開されているものとする。また、例えば、新規取引業者である属性情報受信装置５０は、Ｈ(ＶＩＤ)のリスト中で自分の持つ仮想ＩＤが何番目であるかを知ることができる。

【００４３】

これで、上記のＯＴプロトコルによって、Ｈ(ＶＩＤ)番目のレコードを取得することができる。但し、このままでは、自分の持っている仮想ＩＤに対応するＨ(ＶＩＤ)番目以外を指定してくることがあり、これを防ぐためには、別のハッシュ関数Ｈ'()を用い、予め仮想レコードの属性をＨ'（ＶＩＤ)を鍵として暗号化しておく。このハッシュ関数Ｈ'のアルゴリズムも公開されているものとする。まとめると以下のように構成される。
例えば、仮想レコードが以下のようにｍ個の属性からなっていたとする。
$\{VID_i , Attr_{i,1}, .., Attr_{i,m}\}$
これをk_I ＝ Ｈ'（VID_i）として、属性を暗号化して以下のようにする。
$s_i = \{H(VID_i), E_{k_i}(Attr_m1), ..., E_{k_i}(Attr_m)\}$
そして、Ｈ(VID_i)をキーとして、仮想レコード全体をソートし、順番を割り振り、これに対してＯＴ($\{s_1,..,s_n\}$)を行えばよい。
属性情報受信装置５０では、例えば、ユーザ装置３０から得た仮想ＩＤに基づいて、仮想レコード
$s_i = \{H(VID_i), E_{k_i}(Attr_m1), ..., E_{k_i}(Attr_m)\}$
を取得することができる。これをk_i=Ｈ'（VID_i)によって復号することによって、ｍ個の属性を得ることができる。

【００４４】

以上、詳述したように、本実施の形態では、まず、加入者であるユーザ装置３０は、所定のブラウザを用い、ネットワーク７０を介して個人情報取り扱い業者の運営する属性情報提供サーバ１０に入るように構成した。そして、属性情報提供サーバ１０上のデータベース２０に格納された個人属性テーブルから、必要情報だけを抜き出したものを仮想レコードとして登録し、これのキーとして仮想ＩＤを発行してもらうように構成した。その後、ユーザ装置３０は仮想ＩＤと認証に必要な情報とを新規取引者である属性情報受信装置

５０に送り、属性情報受信装置５０では、その仮想ＩＤを使って、属性情報提供サーバ１０にログインしている。そして、属性情報受信装置５０は、仮想レコードに登録された情報データを属性情報提供サーバ１０から得ることで、属性データを参照し、取引相手が信頼できるかを判断して、取引を開始することが可能となる。

【００４５】

尚、このプロトコルにおけるセキュリティの要件として、

（１）　ユーザ装置３０は、属性情報提供サーバ１０上の自分の属性レコードだけを読むことができる。

（２）　ユーザ装置３０は、仮想レコードを登録する際に、元の属性レコード(ＧＩＤレコード)の中の任意の属性をコピーすることはできるが、改ざんすることはできない。

（３）　属性情報受信装置５０は、属性情報提供サーバ１０から渡された仮想ＩＤ(＋パスワード)によって、その仮想レコードだけを読むことができる。また、このとき次のプライバシー要件も必要に応じて付加することができる。

（４）　属性情報提供サーバ１０は、属性情報受信装置５０が仮想レコードを取得するときに、それがどの仮想ＩＤなのか、即ち、どのユーザ装置３０の仮想レコードを渡そうとしているのかを知ることができない(知り得ない)。

としている。

上記要件の(１)および(３)は、従来の認証の仕組みを使えば容易に実現される。上記要件の(２)については、次のように仮想レコード登録時のサーバ側のチェックとして実現することが可能である。

【００４６】

また、上述したように、本実施の形態では、属性情報提供サーバ１０上での仮想レコードおよび仮想ＩＤの発行は、以下のようになされる。

（１）　個人情報レコードは、ＧＩＤというＩＤをプライマリーキーとして、データベース２０上に登録されているものとする。

（２）　加入者であるユーザ装置３０は、ＧＩＤとは無関係な仮想ＩＤ(ＶＩＤ)をキーとする空のレコードを作る。

（３）　加入者であるユーザ装置３０は、自分のＧＩＤレコードのうち、取引相手(属性情報受信装置５０)に開示したい属性部分だけを仮想ＩＤのレコードにコピーする。

（４）　このとき、属性情報提供サーバ１０は、オリジナルのレコードの属性部と仮想レコードの属性部のＯＲを計算し、この結果がオリジナルレコードの属性部と等しいことを検証する。即ち、

Attribute(GID) OR Attribute(VID) ＝ Attribute(GID)

また、この要件(４)については、暗号技術ＯＴによって実現される。

【００４７】

以上のような構成によって、本実施の形態では、個人情報を持つ機関(属性情報提供サーバ１０)が、その個人の求めに応じて、個人情報の一部を第三者に提供しており、この個人情報を持つ機関は、それを提供するビジネス展開が可能となる。また、加入者(ユーザ装置３０)は、インターネット(ネットワーク７０)上で必要な与信を簡単に得ることができる。個人情報を持つ機関(属性情報提供サーバ１０)としては、金融機関やＩＳＰ(Internet Service Provider)、ネット上の商店サイト等でもよく、加入者(ユーザ装置３０)の同意の下に個人情報を発行するので、プライバシーの問題も生じない。また、新規取引業者(属性情報受信装置５０)が、渡された情報を十分な与信情報と見るか否かは、新規取引業者(属性情報受信装置５０)の任意である。更に、個人情報取り扱い業者(属性情報提供サーバ１０)は、開示する情報については、それが自らが持つ情報と同等である(改ざんされていない)ことだけが責任範囲となり、与信情報そのものについての正当性の保障をする必要がない。例えば、加入者(ユーザ装置３０)が自分の情報の登録時に虚偽の情報を登録した場合の正当性の保証をするものではない。

【００４８】

また、本実施の形態によれば、属性レコード自体が、加入者(ユーザ装置３０)と個人情

報取り扱い業者(属性情報提供サーバ１０)の共有物(加入者自身が登録した属性と、預金額などの活動履歴情報)であることから、加入者(ユーザ装置３０)は、属性情報提供サーバ１０上の自分の属性レコードだけを読むことができる。また、加入者(ユーザ装置３０)は、仮想レコードを登録する際に、元の属性レコードの中における任意の属性をコピーすることはできるが、改ざんすることはできない。これによって、加入者は、名前を特定されずに預金額などの属性だけを証明することが可能となる。更に、新規取引者(属性情報受信装置５０)は、加入者(ユーザ装置３０)から渡された仮想ＩＤ(＋パスワード)によって、その仮想レコードだけを読むことができる。即ち、新規取引者(属性情報受信装置５０)側にて認証は仮想ＩＤだけで行われるので、個人情報取り扱い業者(属性情報提供サーバ１０)は、だれが仮想レコードをアクセスしたかを知ることができない。その結果、この仮想ＩＤの受け渡しは、加入者(ユーザ装置３０)の責任であることが明確化される。また更に、個人情報取り扱い業者(属性情報提供サーバ１０)は、1-out-of-N OTによって、どの加入者(ユーザ装置３０)の仮想ＩＤを要求されているのかを知り得ない。これによって、加入者(ユーザ装置３０)は、自分がどの新規取引業者(属性情報受信装置５０)と取り引きしようとしているかを、個人情報取り扱い業者(属性情報提供サーバ１０)に知られない状態で、認証だけを受けることができる。これによって、加入者(ユーザ装置３０)のプライバシーの保護が強化され、また、個人情報取引業者(属性情報提供サーバ１０)にとっても、不必要な情報を知ることなく、サービスすることが可能となる。

【産業上の利用可能性】

【００４９】

本発明の活用例としては、属性情報提供サーバとして用いられるサーバ、ユーザ装置や属性情報受信装置として用いられるＰＣなどのコンピュータ装置などがあり、これらをインターネットなどのネットワークを介してＷｅｂ接続されたシステム構成が考えられる。サービスプロバイダとして適用される属性情報提供サーバは、ＩＳＰ(Internet Service Provider)や金融機関、ショップサイトなどが考えられる。サービスプロバイダとしての社会的信頼が高ければ高いほど、その与信サービスも価値あるものとなる。

【図面の簡単な説明】

【００５０】

【図１】本実施の形態が適用される属性情報提供システム(与信付与システム)の全体構成を示した図である。

【図２】属性情報提供システムの各装置が実行する処理を示したフローチャートである。

【図３】本実施形態の属性情報提供サーバやユーザ装置、属性情報受信装置を実現するのに好適なコンピュータ装置のハードウェア構成例を模式的に示した図である。

【図４】本実施形態の属性情報提供サーバにおける機能構成を示した図である。

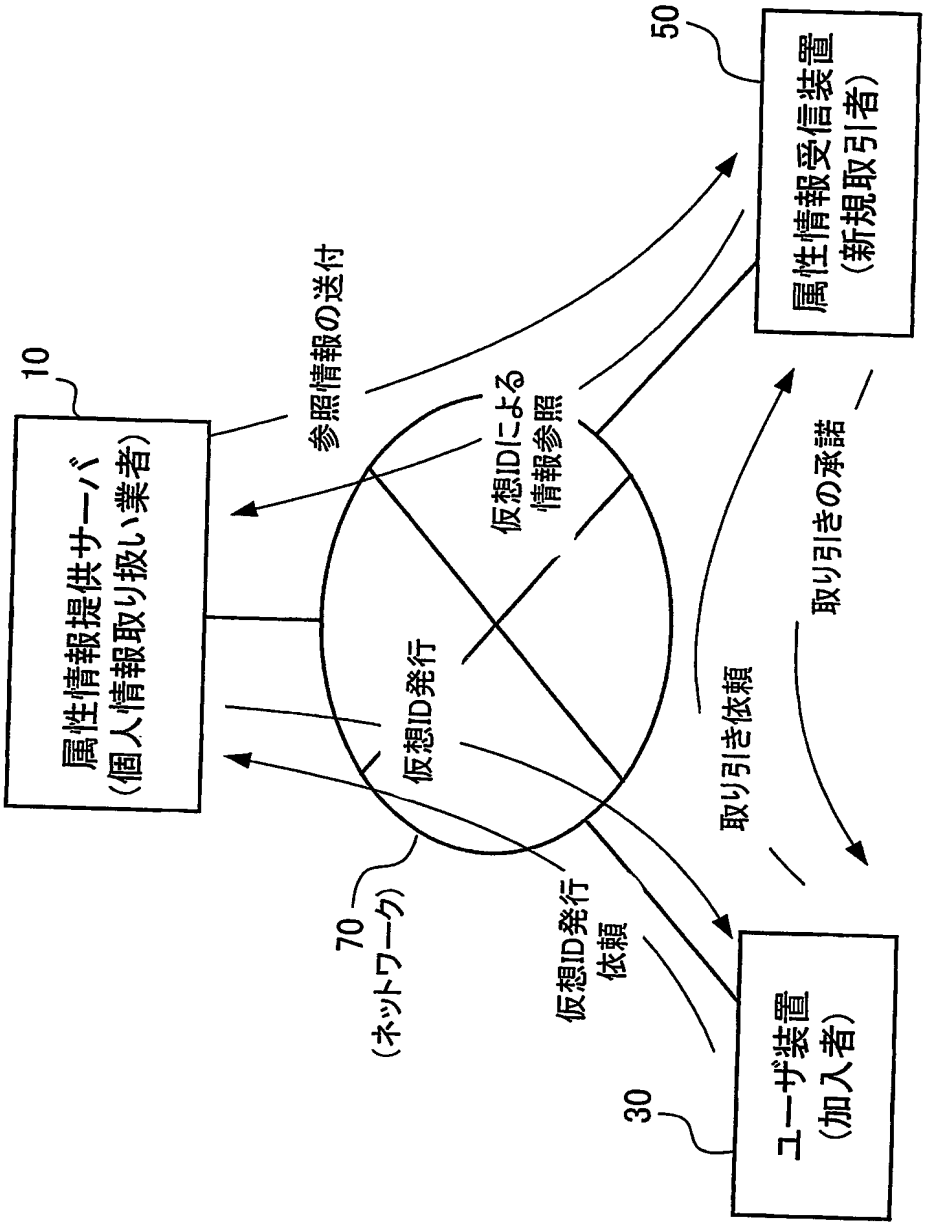
【図５】ユーザ装置のディスプレイに表示される顧客レコードおよび仮想レコードの例を示した図である。

【符号の説明】

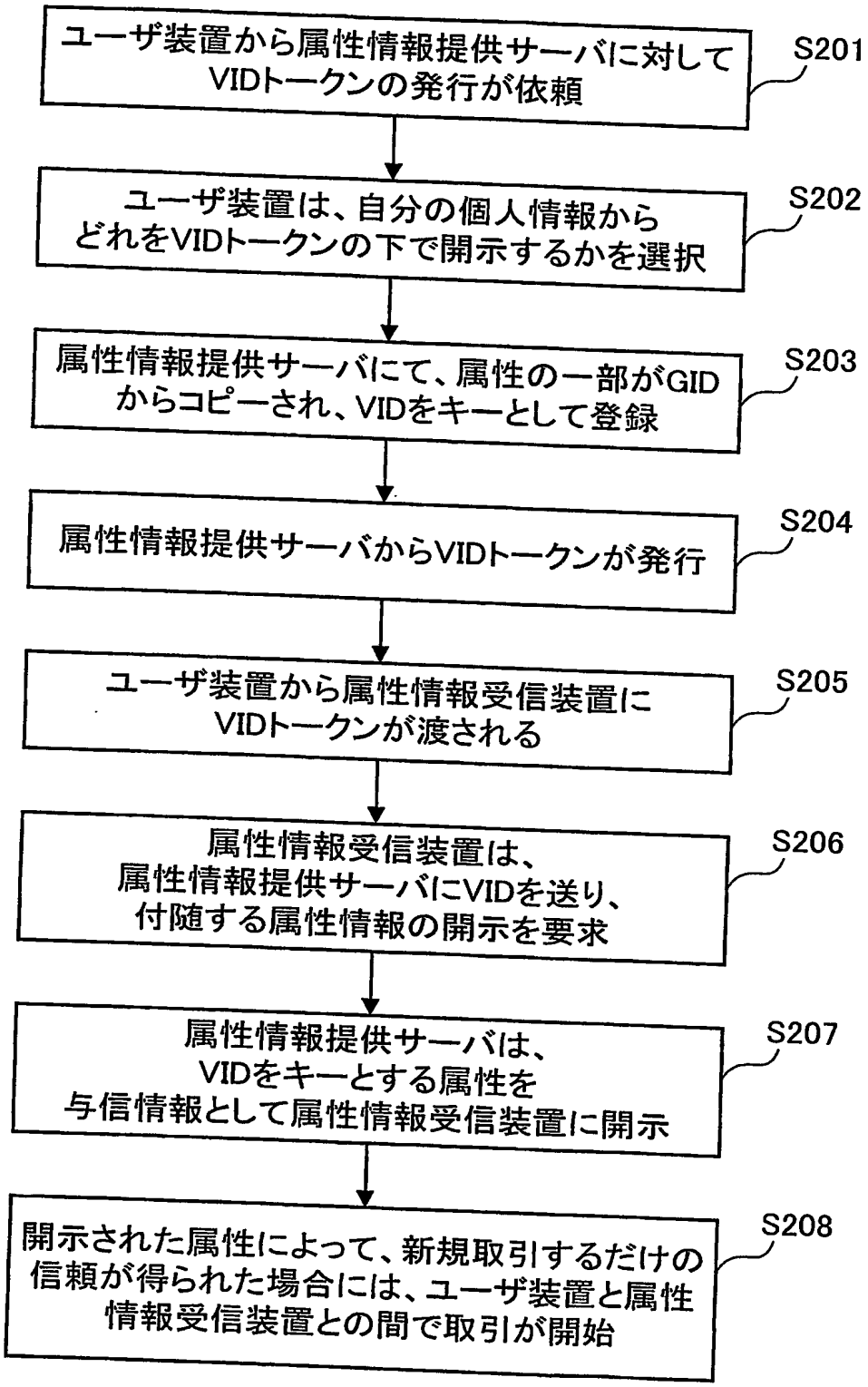
【００５１】

１０…属性情報提供サーバ(個人情報サーバ)、１１…顧客レコード表示部、１２…属性選択部、１３…仮想レコード生成部、１４…ＶＩＤトークン発行部、１８…仮想レコード参照処理部、１９…仮想レコード発行部、２０…データベース、３０…ユーザ装置、５０…属性情報受信装置(与信情報受信装置)、７０…ネットワーク

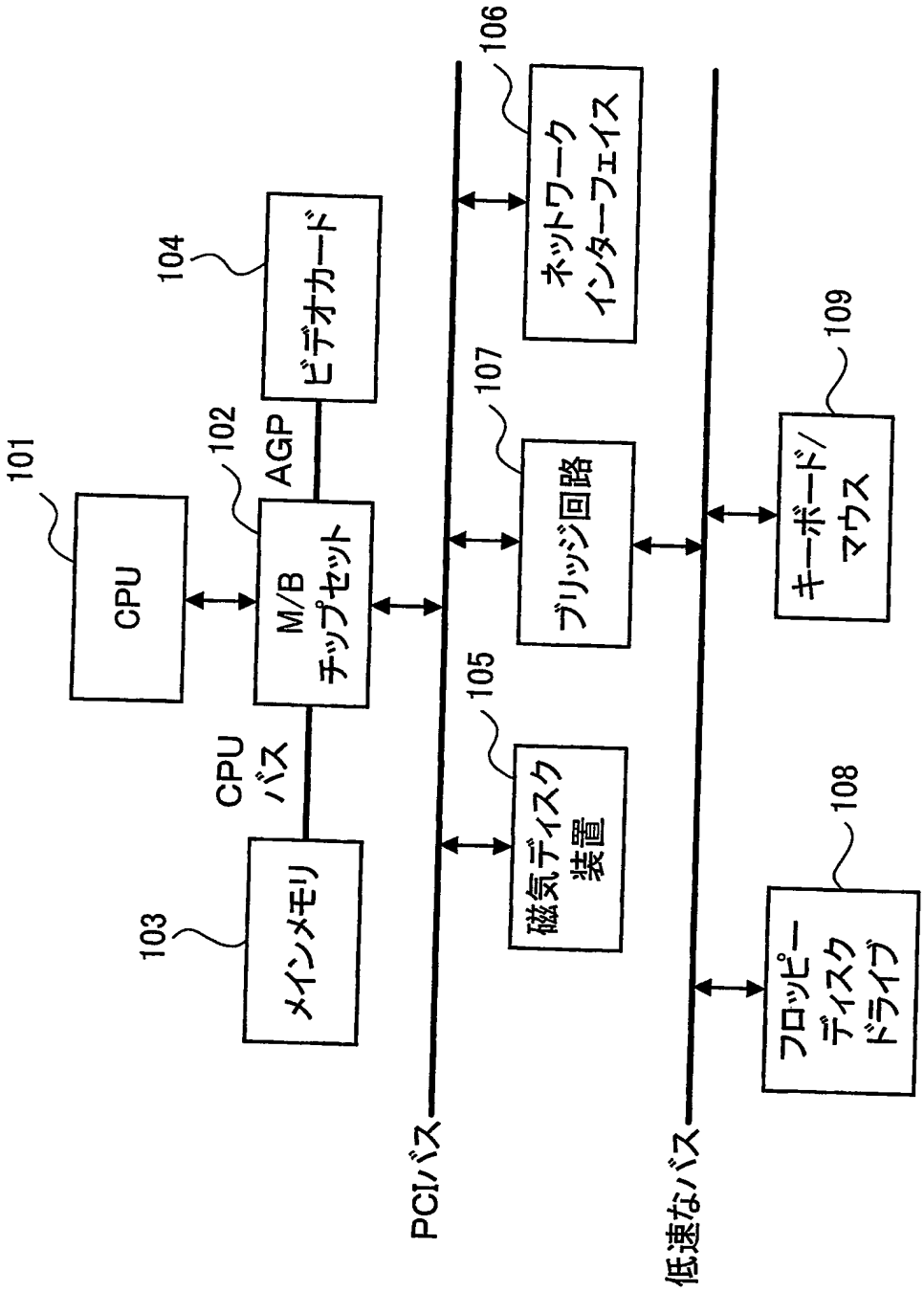
【書類名】図面
【図１】


10
属性情報提供サーバ
（個人情報取り扱い業者）
参照情報の送付
仮想IDによる
情報参照
50
属性情報受信装置
（新規取引者）
仮想ID発行
70
（ネットワーク）
仮想ID発行
依頼
取り引き依頼
取り引きの承諾
30
ユーザ装置
（加入者）

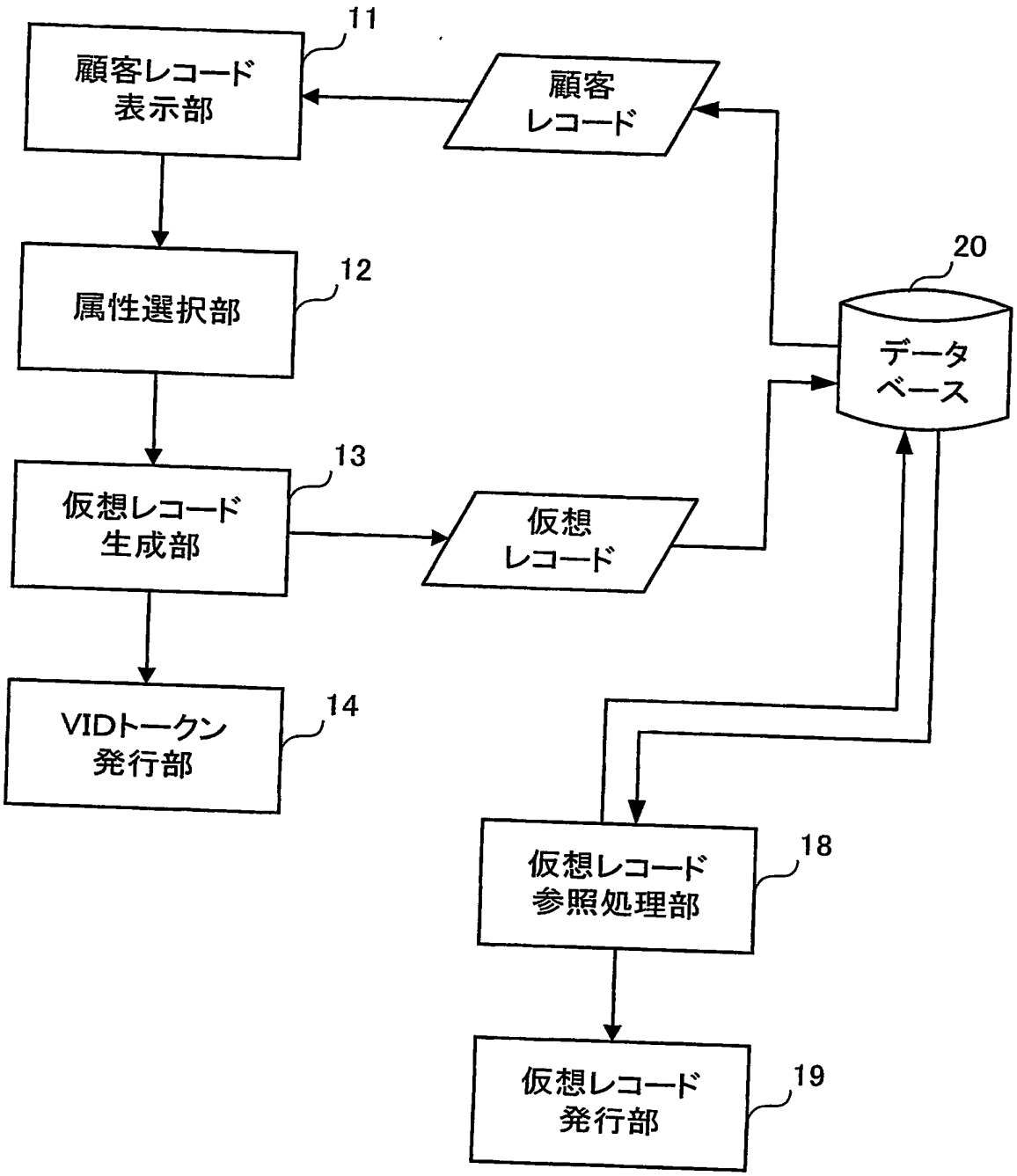
【図２】


ユーザ装置から属性情報提供サーバに対して
VIDトークンの発行が依頼
S201
ユーザ装置は、自分の個人情報から
どれをVIDトークンの下で開示するかを選択
S202
属性情報提供サーバにて、属性の一部がGID
からコピーされ、VIDをキーとして登録
S203
属性情報提供サーバからVIDトークンが発行
S204
ユーザ装置から属性情報受信装置に
VIDトークンが渡される
S205
属性情報受信装置は、
属性情報提供サーバにVIDを送り、
付随する属性情報の開示を要求
S206
属性情報提供サーバは、
VIDをキーとする属性を
与信情報として属性情報受信装置に開示
S207
開示された属性によって、新規取引するだけの
信頼が得られた場合には、ユーザ装置と属性
情報受信装置との間で取引が開始
S208

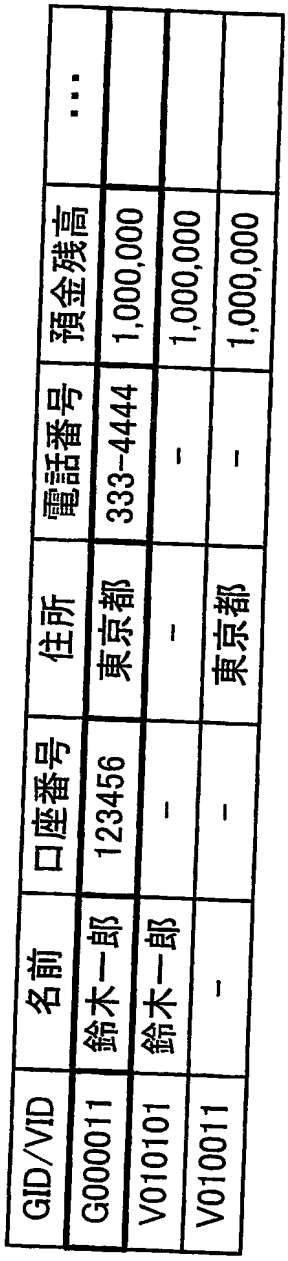
【図３】


101
CPU
102
M/B
チップセット
AGP
104
ビデオカード
CPU
バス
103
メインメモリ
PCIバス
105
磁気ディスク
装置
106
ネットワーク
インターフェイス
107
ブリッジ回路
109
キーボード/
マウス
低速なバス
108
フロッピー
ディスク
ドライブ

【図４】


11
顧客レコード
表示部
顧客
レコード
12
属性選択部
20
データ
ベース
13
仮想レコード
生成部
仮想
レコード
14
VIDトークン
発行部
18
仮想レコード
参照処理部
19
仮想レコード
発行部

【図５】



GID/VID	名前	口座番号	住所	電話番号	預金残高	...
G000011	鈴木一郎	123456	東京都	333-4444	1,000,000	
V010101	鈴木一郎	-	-	-	1,000,000	
V010011	-	-	東京都	-	1,000,000	

【書類名】要約書

【要約】

【課題】　個人情報を持つ個人情報取り扱い業者が、その個人の求めに応じて個人情報の一部を第三者に提供し、個人情報取り扱い業者および個人の双方に利益のあるビジネスを提供する。

【解決手段】　加入者の個人情報が格納されたデータベースから所定の個人情報をネットワーク７０を介して提供する属性情報提供サーバ１０と、属性情報提供サーバ１０に対して加入者自らの個人情報の中から幾つかの情報を抜き出すユーザ装置３０と、属性情報提供サーバ１０からユーザ装置３０を利用する加入者に関する所定の個人情報を取得する属性情報受信装置５０とを備え、属性情報提供サーバ１０は、ユーザ装置３０によってデータベースから抜き出された幾つかの属性情報だけを仮想レコードとしてデータベースに登録すると共に、この仮想レコードのキーとしての仮想ＩＤをユーザ装置３０に提供し、属性情報受信装置５０は、仮想ＩＤをユーザ装置３０から取得し、この仮想ＩＤに基づいて属性情報提供サーバ１０から仮想レコードを読み込む。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－３０４８８２
受付番号	5.03014268 27
書類名	特許願
担当官	土井　恵子　　４２６４
作成日	平成１５年　８月２９日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 592073101
- 【住所又は居所】 東京都港区六本木３丁目２番１２号
- 【氏名又は名称】 日本アイ・ビー・エム株式会社

【代理人】
- 【識別番号】 100086243
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 坂口　博

【代理人】
- 【識別番号】 100091568
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 市位　嘉宏

【代理人】
- 【識別番号】 100108501
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社　知的所有権
- 【氏名又は名称】 上野　剛史

【復代理人】 申請人
- 【識別番号】 100104880
- 【住所又は居所】 東京都港区赤坂５－４－１１　山口建設第２ビル６Ｆ　セリオ国際特許事務所
- 【氏名又は名称】 古部　次郎

【選任した復代理人】
- 【識別番号】 100118201
- 【住所又は居所】 東京都港区赤坂５－４－１１　山口建設第二ビル６Ｆ　セリオ国際特許事務所
- 【氏名又は名称】 千田　武

特願２００３－３０４８８２

出　願　人　履　歴　情　報

識別番号　［５９２０７３１０１］

１．変更年月日　１９９２年　４月　３日
［変更理由］　新規登録
住　所　東京都港区六本木３丁目２番１２号
氏　名　日本アイ・ビー・エム株式会社